



April 13, 2004

Ms. Debbie Gundersen
State of Utah
Division of Purchasing
State Office Building, Room 3150
Salt Lake City, Utah 84114

Dear Ms. Gundersen:

Ecutel Systems, Inc. is pleased to present to the State of Utah our Best and Final Offer (BAFO) in connection with the Request for Proposal for the Networking System for Application Persistence.

In addition to clarifying your technical questions, this BAFO includes more favorable pricing for small State agencies than the original proposal. The subscription-based pricing offer, which was submitted under a separate proposal, still stands.

I will serve as the authorized representative of Ecutel Systems, Inc. for all matters relating to this proposal. I have included my contact information for your convenience:

Name:	Kevin Hayes
Title:	Vice President, Federal & State Government
Address:	2300 Corporate Park Drive – Suite 410 Herndon, VA 20171
Office Phone:	571-203-8335
Cellular Phone:	703-850-8963
Facsimile:	571-203-8310
Email:	<u>khayes@ecutel.com</u>

We appreciate the opportunity to submit our responses and look forward to the success of your project.

Sincerely,

Kevin Hayes



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

BEST AND FINAL OFFER

April 7, 2004

VIA: email
lwagner@ecutel.com

Larry Wagner
Ecutel Systems, Inc.
2300 Corporate Park Drive, Suite 410
Herndon, VA 20171

RE: BEST AND FINAL OFFER REQUEST (BAFO)
RFP DG4009, Contract for Networking System for Application Persistence

Dear Larry:

The evaluation of the responses to the Request for Proposal DG4009 has been completed. After an extensive review, the Division of Purchasing is requesting a Best and Final Offer and requests your detailed response on the following items:

5.10 Revision to Question:

What are some scenarios that require preconfiguration of parameters? Please provide some examples with their respective parameter settings.

Ecutel Response: Please see Appendix A

5.11 Revision to Question:

What types of user-specific information is stored locally on the client PC? What settings, if any, can be modified by the end user?

Ecutel Response: Please see Appendix A

5.14 Revision to Question:

Are there custom implementations required where Novell Netware clients are in use? What steps, if any, are required to bring the laptop into compliance, so the network persistence software will function on these laptops? Is there additional software, which must be loaded, or is there software that must be removed from these laptops?

Ecutel Response: Please see Appendix A



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

5.16 Revision to Question:

Some applications, using telnet sessions, need to remain active during network transitions. Please confirm that these types of sessions, as well as other Windows-based applications, will not be disrupted due to the network switching indicated above.

Ecutel Response: Please see Appendix A

5.17 Addendum to Question:

Please explain in more detail how your product prioritizes active network connections, and enables automatic switching to the highest speed network connection.

Ecutel Response: Please see Appendix A

Offerors must respond to these items using the same format as they did when responding to the original RFP. Also at this time, you may offer any clarifications or enhancements that you would like to your original submission including your pricing. It must be in the same format as the original requirements and must be clearly identified per section.

The Best and Final Offer response is due in a sealed envelope by 5:00 p.m. on Wednesday April 14, 2004. One (1) Original, five (5) identical hard copies and one (1) electronic copy of the BAFO are required. Send your response to the Division of Purchasing and General Services, 3150 State Office Building, Capitol Hill, Salt Lake City, UT 84114, attn. Debbie Gundersen. If you do not submit a notice of withdrawal or a Best and Final Offer, your immediate previous offer will be construed as your Best and Final Offer.

With Questions relative to this BAFO process please contact me at 801-538-3150.

Sincerely,

Debbie Gundersen

Debbie Gundersen, C.P.M.
Purchasing Agent



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services
S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services
DOUGLAS RICHINS
Division Director

Section 6.0 BAFO Pricing Due: April 14, 2004

6.1 Price Quote Information General

The vendor shall provide a detailed itemized price quote for a statewide enterprise system as well as pricing for scalable solutions that would allow for smaller agencies within the State of Utah to deploy stand-alone systems. The number of State users cannot be guaranteed, but could potentially increase to 2,000 over the next five years.

6.2 Enterprise System Pricing

Provide a price for an enterprise system as identified in your technical offer, as well as pricing for stand-alone systems should State agencies choose to implement a system separate from an ITS-deployed system. This price must include the first year maintenance and support fees. Provide pricing as follows:

Ecutel Response:

Client Licensing Fee (incl. 1 st Year Maintenance)	Total	25 Client Pack Pricing*
Licensing Fee for up to 100 clients:	\$ 10,436	\$ 2,609
Licensing Fee for up to 500 clients:	\$ 50,860	\$ 2,543
Licensing Fee for up to 1000 clients:	\$ 99,120	\$ 2,478
Licensing Fee for up to 5000 clients:	\$ 482,600	\$ 2,413
Licensing Fee for up to 10,000 clients:	\$ 939,200	\$ 2,348
Licensing Fee Application Hosting Software (Primary) [†] :	\$ 10,000	
Licensing Fee Application Hosting Software (Secondary) [‡] :	\$ 5,000	

* Clients are sold in blocks of 25 and pricing is set based on the cumulative volume of Clients sold to the State of Utah and its agencies.

[†] One Primary Hosting Server must be purchased by the State of Utah.

[‡] Secondary Hosting Servers can be used for as fail-over servers for large implementation or can be purchased by small agencies within the State of Utah as stand-alone servers.



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

Client Licensing Fee (incl. 1 st Year Maintenance)	Total	25 Client Pack Pricing*
System Hardware:		
Other: Acceleration PCI card (SafeXcel™ 141-PCI)/each	\$ 1,500	
Other: Acceleration PCI card (SafeXcel™ 241-PCI)/each	\$ 1,000	

Enterprise-wide Pricing Example:

Component	Cost
1 Server	\$10,000
500 Clients	\$50,860
PCI-141 Card (Recommended)	\$1,500
Total	\$62,360

Small Agency Pricing Example:

After the first enterprise-wide purchase, the Small Agency would qualify for purchasing a secondary server at \$5,000 and a block of 25 Clients at the state-wide volume discount.

Component	Cost
1 Server	\$5,000
25 Client Pack	\$2,478
Total	\$7,478

Additionally, each purchase of Client Licenses by qualifying Small Agencies will accumulate toward the total number of Statewide Client Licenses purchased for purposes of volume pricing discounts.

All pricing is for the latest release of Viatores (version 4.4) which offers the following enhancements:

- **FIPS (Federal Information Processing Standard)-certified cryptographic hardware acceleration support with encrypted throughput of up to 290 Mbps.**
- **Advanced Encryption Standard (AES) Support.** AES is the latest encryption standard developed by the National Institute for Standards and Technology (NIST) and approved under publication number FIPS-197 for use by Federal agencies to encrypt sensitive information.



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services
S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services
DOUGLAS RICHINS
Division Director

- **Advanced traffic control policies.** These new policies give network administrators the ability to centrally control which applications are allowed to run on the mobile device based on the wired or wireless network to which the device is connected. This helps enterprises enforce wired and wireless network usage, preserve network bandwidth, and reduce usage costs.
- **Advanced Client-Server Compression.** Viatores' new compression feature can be enabled to dramatically improve the throughput of low bandwidth networks. Compression in Viatores is performed prior to encryption to lower packet sizes, reduce packet latency, and increase overall performance.

6.3 Ongoing Maintenance and Support

Provide pricing for maintenance and support fees for second year, and for the three optional renewal periods of product license.

Ecutel Response:

The maintenance fee is based on total software deployed per location and includes both support and upgrades. The first year's maintenance is included in the above pricing. The following discounts will be applied when purchasing maintenance with the original Purchase Order.

One Year Prepaid (Second year)	18% per year
Two Years Prepaid (Second & Third Year)	15% per year
Three or More Years Prepaid (Fourth Year or more)	10% per year

6.4 Training

Provide pricing for any training recommended. Specify location, rates, and incidental costs.

Ecutel Response:

Ecutel Systems, Inc. offers the Viatores Basic Class. On-site training is provided by the professional consulting services organization and is available plus travel and expenses. Viatores Basic Technical Training course: Provide an overview of networking protocol



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

standards (MIP, IPSec, Routing, DHCP, PPP, Wired and Wireless protocols); Viatores components; Viatores mobility, security and connectivity capabilities; Administrator and User configuration, product installation and fielding; hands-on class room practice. This is a 2-day class.

On Site Training

\$ 1,000/day*

Headquarters Training

\$ 500/day

Headquarters Address

Ecutel Systems, Inc.
2300 Corporate Park Drive Suite 410
Herndon, VA 20171

**Professional Services (i.e. installation, training and consulting) does not include travel and other expense. All travel will be invoiced at cost based on travel from our Virginia office. With any Purchase Order over \$25,000, the travel fee will be waived for professional services for the first site visit.*

6.5 Consulting Services

If consultant services are offered to support the software, list the name, job title, and hourly rate for any proposed consultant:

Ecutel Response:

Name: Mark Mazur Title: Project Engineer \$ 1,500/day on site*

Name: Dzung Tran Title: CTO/Custom Development \$ 200/ hour headquarters

**Professional Services (i.e. installation, training and consulting) does not include travel and other expense. All travel will be invoiced at cost based on travel from our Virginia office. With any Purchase Order over \$25,000, the travel fee will be waived for professional services for the first site visit.*



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

Appendix A

5.10 Revision to Question:

What are some scenarios that require preconfiguration of parameters? Please provide some examples with their respective parameter settings.

Ecutel response:

The Viatores system provides pre-configuration steps as a means to enable the system administrator to implement strong security access to the enterprise network and mobile devices while still providing ease-of-use for mobile users. There are two types of configuration:

- I) Mobile device installation configuration
- II) System wide policy configuration

During installation of Viatores Client software on the mobile device, the system administrator can run an interactive installer, as depicted in figure 5.10-1 below, or create a batch installation file to run such installer with parameters on the command line to fit the mobile laptop environment requirements. After the installation process is completed using either interactive or batch method, these preconfiguration parameters are stored in proper registry entries for access by the Viatores Client during operational use.



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director



Figure 5.10-1- Interactive installation screen

The following examples illustrate such batch installation:

```
msiexec /I Viatores.msi PIDKEY="4589204074-2907D67235"  
USERNAME="Capt Smith" COMPANYNAME="State of Utah"
```



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

The above example specifies the product's serial string, the User Name, and the Company Name.

```
msiexec /q /I Viatores.msi PIDKEY="4589204074-2907D67235"  
USERNAME="Capt Smith" COMPANYNAME=" State of Utah"  
STARTUPMETHOD=0 DRIVERINSTALLED=FALSE
```

The above example specifies the product's serial string, the User Name, and Company Name. It also sets the startup method to Manual and installs the Client in silent mode.

```
msiexec /I Viatores.msi REINSTALL=All REINSTALLMODE=vomus
```

The above example specifies that Viatores Client has already been installed should be reinstalled completely.

```
msiexec /I Viatores.msi PIDKEY="4589204074-2907D67235"  
REINSTALL=ALL REINSTALLMODE=vomus
```

The above example specifies that a product that is already installed should be upgraded to a newer version of the product.

Since the mobile device installation can be installed using files with extension in .MSI or .EXE, the system administration can customize installation through the use of Microsoft MSI installation environment, System Management Server (SMS) to distribute user and group policy or login script to allow users to access the Viatores Client while maintaining clear separation of local administrator account and restricted user account access, thus avoiding intentional or unintentional changing of the mobile device environment.

The following table 5.10-2 describes all possible flags that can be specified during Viatores Client installation on the mobile device to customize Client environment.



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

PIDKEY	Serial string	The product's serial string provided to you by the manufacturer.
STARTUPMETHOD	0 1 2 4	<p>Specify the method used to start the Viatores Client after it is installed:</p> <p>0 – Manual. User will start the Client manually from the Start menu.</p> <p>1 – Automatic. The Client will start automatically after Windows starts.</p> <p>2 – Single Sign-On. The Client startup process is integrated with the Windows startup process.</p> <p>4 – Smartcard. A smartcard will be used to start the Client.</p> <p>If no option is selected, the default is set to 2.</p>
USERNAME	User's name	The name of the user that will use the Viatores Client.
COMPANYNAME	Company name	The name of the organization that will use the Viatores Client.
RCUSERNAME	Admin Username	<p>The username of a member of the local Windows Administrator Group.</p> <p>This parameter is required if ALLOWACCESS is set to Yes.</p>
RCPASSWORD	Admin Password	<p>The password of a member of the local Windows Administrator Group.</p> <p>This parameter is required if ALLOWACCESS is set to Yes.</p>
STARTBYDEFAULT	Yes No	Enables the Start Viatores on login checkbox to be checked by default on the Windows login screen.



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

ALLOWBYPASS	Yes No	<p>Prevents the user from bypassing the Viatores Client at login. If this option is selected, the user will be required to login using Viatores each time:</p> <p>Yes – Prevent the user from bypassing the Client at login.</p> <p>No – Allow the user to bypass the Client at login.</p> <p>This option is required if STARTUPMETHOD is set to 2 (Single Sign-On) only.</p> <p>If this option is set to Yes, the STARTBYDEFAULT option is set to Yes automatically.</p>
REQUIREPASSWORD	Yes No	<p>Prevent the Client user from maximizing the Viatores Client window unless the Viatores password is entered:</p> <p>Yes – Require password to maximize the Client window.</p> <p>No – Do not require password to maximize the Client window.</p>
ALLOWACCESS	Yes No	<p>Allow Standard/Restricted users access. By default, these users do not have the correct privileges to switch network devices.</p> <p>Yes – Enable users who are not members of the local Windows Administrators Group to use the Viatores Client. If selected, RCUSERNAME and RCPASSWORD must be specified.</p> <p>No – Non-Administrative users will not be allowed to use the Viatores Client.</p>
TARGETDIR	Folder location	<p>The location where the Viatores Client should be installed on the local machine. The default value, C:\Program Files\Ecutel\Viatores Client, will be used if this property is not specified.</p>



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

REBOOT	Force Suppress	<p>Sets the option to reboot the machine at the end of the installation. A reboot is required for the Viatores Client installation to function properly. However, the user can be allowed to reboot the machine at a later time, if desired:</p> <p>Force – Always prompt for a reboot at the end of the installation. The UI always prompts the user with an option to reboot at the end. If there is no user interface (e.g. silent installation) the system automatically reboots at the end of the Client installation. This is the default value.</p> <p>Suppress – Suppress the prompt for a reboot at the end of the Client installation. If there is no user interface (e.g. silent installation), the installer will not reboot. Please note that when specified, the user must reboot the machine in order for the Viatores Client to function properly.</p>
REINSTALL	All	<p>Specifies the features of Viatores to be reinstalled. The only supported option is All.</p>
REINSTALLMODE	o m u s v	<p>o – Reinstall if file is missing, or an older version is present.</p> <p>m – Rewrite all required registry entries from the Registry table that go to the HKEY_LOCAL_MACHINE or HKEY_CLASSES_ROOT registry hive.</p> <p>u – Rewrite all required registry entries from the Registry table that go to the HKEY_CURRENT_USER or HKEY_USERS registry hive.</p> <p>s – Reinstall all shortcuts and re-cache all icons overwriting any existing shortcuts and icons.</p> <p>v – Use to run from the source package and re-cache the local package. Do not use the v reinstall option code for the first installation of an application or feature.</p> <p>When reinstalling Viatores, it is recommended that you specify all five parameters.</p>

Table 5.10-2 – Pre-configurable parameters for batch installation



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

After installation and policy import, the Client system registry editor contains appropriate parameters to enable enforcement of Viatores security and mobile access.

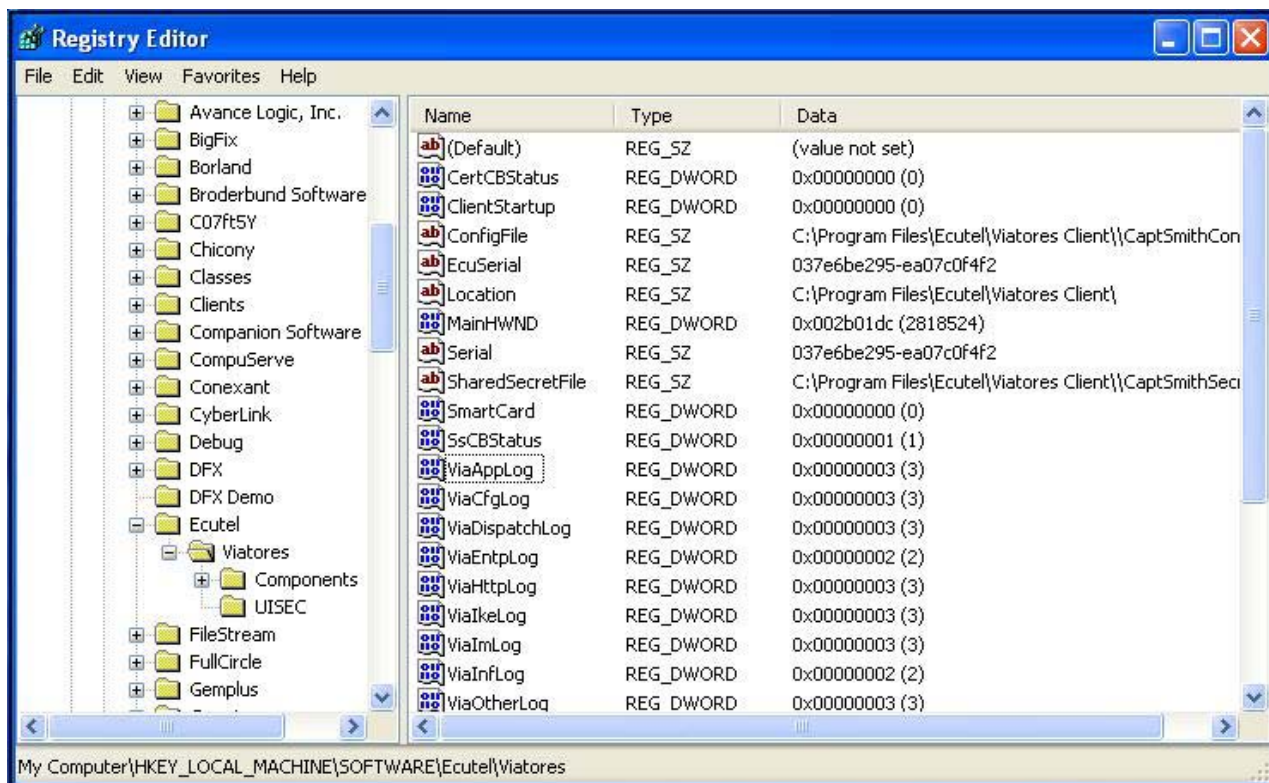


Figure 5.10-3 – Registry pre-configured settings

In terms of configuring and storing system wide mobility and security policy, the system administrator would make use of the Viatores Manager provisioning screens to design such policy and then export the policy to system parameters that can be processed by the Viatores Client. Figures 5.10.3 through 5.10.7 show sample provisioning screens used to create parameters for the mobile device. Once the policy parameters are generated, it is stored in a 3-DES encrypted file. An example of such policy is shown in table 5.10-8. The Viatores Client will follow policy parameters to ensure security is enforced and system access is controlled according the specified authentication method.



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

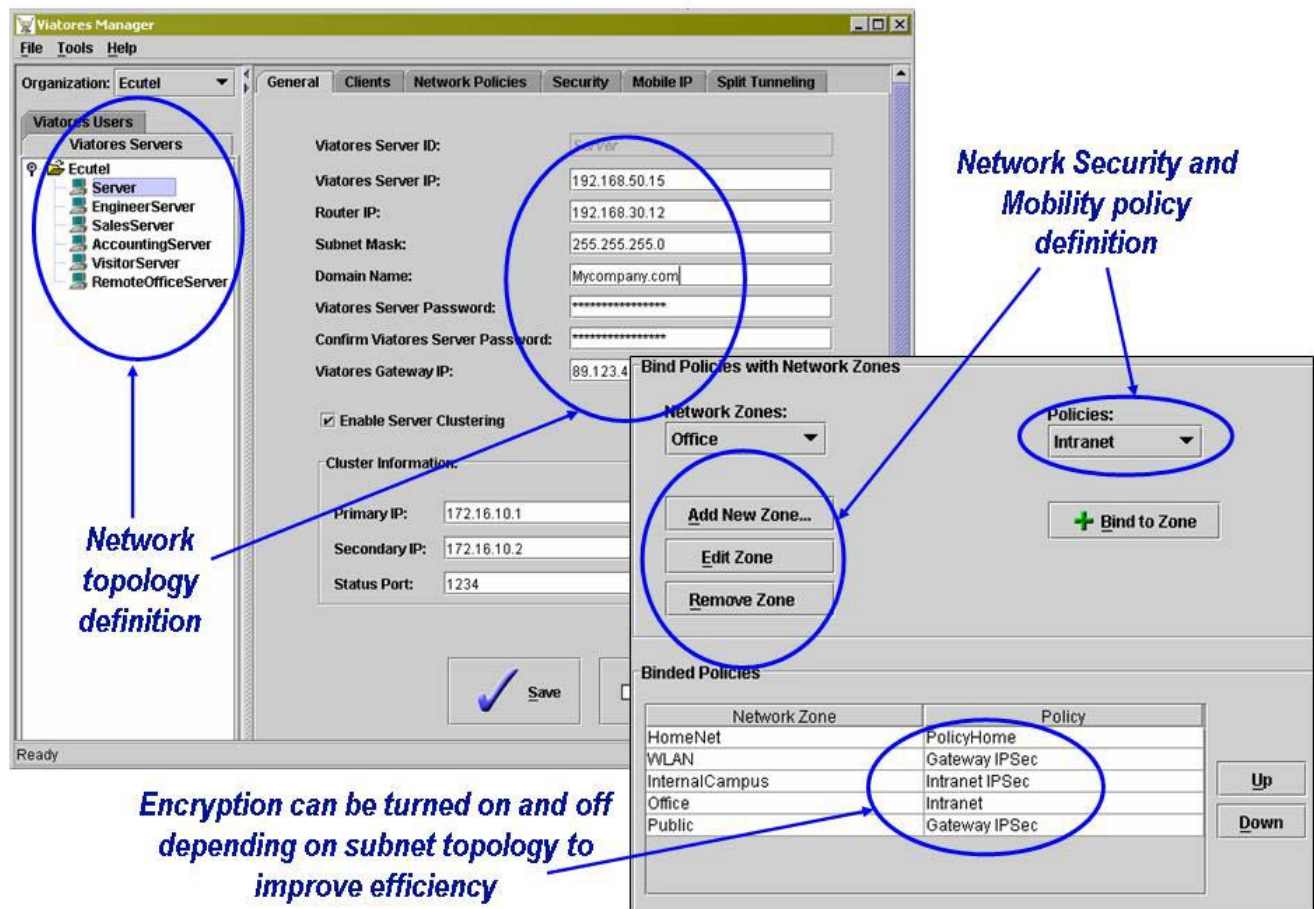


Figure 5-10-4 – Specify network server IP server and router that control mobile devices



State of Utah

OLENE S. WALKER
Governor

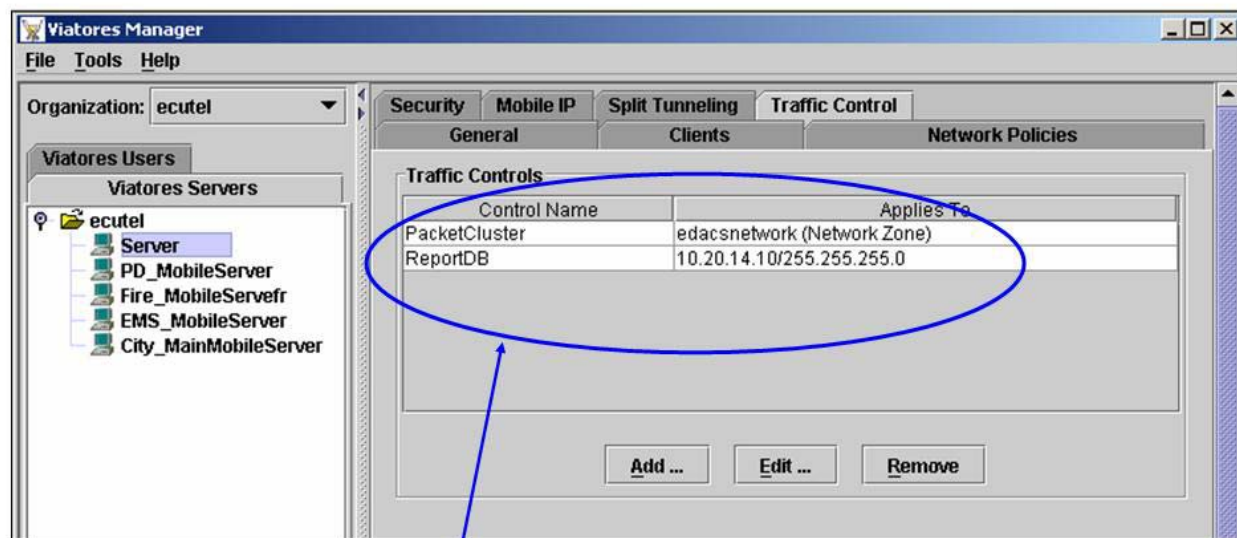
GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director



*Traffic control on specific
interface and protocol for low
bandwidth and security control*

Figure 5.10-5 – How to automatically restrict traffic pattern on a low speed network



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

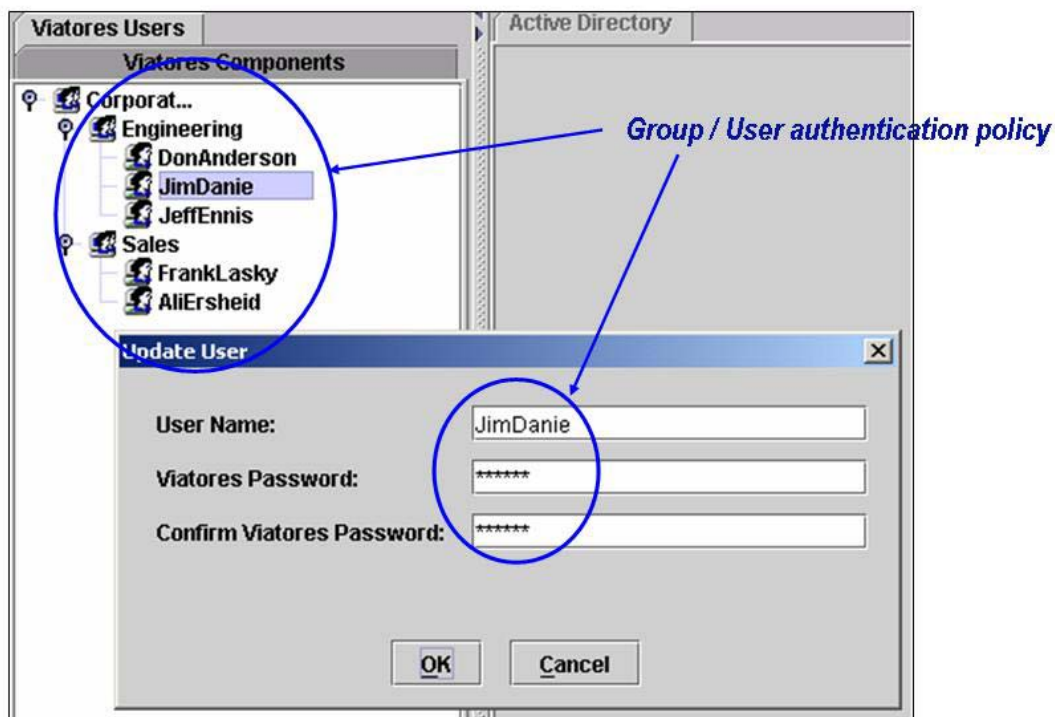


Figure 5.10.6 – How the mobile user authentication is specified and encoded for mobile access

DN	:	HomeNet
ObjectType	:	ViatoresLocation
SubnetAddress	:	192.168.80.0
SubnetMask	:	255.255.255.0
DN	:	Public
ObjectType	:	ViatoresLocation



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

SubnetAddress	:	0.0.0.0
SubnetMask	:	0.0.0.0
DN	:	UDP
ObjectType	:	ViatoresLocation
SubnetAddress	:	0.0.0.0
SubnetMask	:	0.0.0.0
DN	:	AllPackets
ObjectType	:	ViatoresSelector
SelectorType	:	SEL_ALL_PACK
LocalAddrLower	:	0.0.0.0
LocalAddrUpper	:	0.0.0.0
RemoteAddrLower	:	192.168.80.201
RemoteAddrUpper	:	192.168.80.240
LocalAddrFlag	:	FROMPOLICY
RemoteAddrFlag	:	FROMPOLICY
TransProtoFlag	:	FROMPOLICY
LocalPortFlag	:	FROMPOLICY
RemotePortFlag	:	FROMPOLICY
DN	:	RegistrationPacket
ObjectType	:	ViatoresSelector
SelectorType	:	SEL_REG_PACK
LocalPort	:	434
TransportProto	:	UDP
DN	:	IKEPacket
ObjectType	:	ViatoresSelector
SelectorType	:	SEL_IKE_PACK
LocalPort	:	500
TransportProto	:	UDP
DN	:	MipAction
ObjectType	:	ViatoresAction
ActionType	:	MIP
RegLifeTime	:	180
BcastData	:	0
RevTunnel	:	1



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

VJCompress	:	0
GREncaps	:	0
MinEncaps	:	0
UdpEncaps	:	1
SimBinding	:	0
SPI	:	1002
DN	:	PassAction
ObjectType	:	ViatoresAction
ActionType	:	PASS
DN	:	IpSecAction
ObjectType	:	ViatoresAction
ActionType	:	IPSEC
ISAKMPLifeType	:	SECONDS
ISAKMPLifeValue	:	3600
ISAKMPGroup	:	MODP1024
ISAKMPAuthMode	:	PSK
ISAKMPEnc	:	AES
ISAKMPHash	:	SHA
IKEUsePFS	:	1
IPSecLifeType	:	SECONDS
IPSecLifeValue	:	1800
IPSecProto	:	ESP
IPSecEnc	:	AES
IPSecHash	:	SHA
IPSecMode	:	TUNNEL
IPSecGW	:	HOMEAGENT
DN	:	UdpTunnel
ObjectType	:	ViatoresAction
ActionType	:	UDP_TUNNEL
UdpType	:	UDP_REGULAR_TYPE
TimerInterval	:	400
PubHAUdpPort	:	999
MNUdpPort	:	999
PubHAIPAddress	:	14.65.139.23
DN	:	MipActionEnterGate



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

ObjectType	:	ViatoresAction
ActionType	:	MIP_ENTGATE
RegLifeTime	:	180
BcastData	:	0
RevTunnel	:	1
VJCompress	:	0
GREEncaps	:	0
MinEncaps	:	0
UdpEncaps	:	1
SimBinding	:	0
SPI	:	1002
EnterGate	:	14.65.139.23
DN	:	VServer
ObjectType	:	ViatoresEnterprise
Version	:	1
EnterpriseAddress	:	192.168.80.103
RouterAddress	:	192.168.80.1
SubnetAddress	:	192.168.80.0
SubnetNetmask	:	255.255.255.0
PolicyRef	:	PolicyHome
PolicyRef	:	PolicyUDPSUDP
AdminContact	:	support@Utah.gov
DN	:	CaptSmith
ObjectType	:	ViatoresShuttle
Version	:	1
PermanentAddress	:	192.168.80.227
EnterpriseRef	:	VServer
PolicyRef	:	PolicyHome
PolicyRef	:	PolicyUDPSUDP
DomainName	:	Utah.gov
DNS_num	:	1
DNS_IP	:	192.168.80.22
WINS_num	:	1
WINS_IP	:	192.168.80.22
NAI	:	CaptSmith@Utah.gov



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

Table 5.10-7 – Sample subnet of preconfigured policy parameters on the mobile device as a result of provisioning



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services
S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services
DOUGLAS RICHINS
Division Director

5.11 Revision to Question:

What types of user-specific information is stored locally on the client PC? What settings, if any, can be modified by the end user?

Ecutel Response:

The Viatores Client component provides strong security access protection through multiple authentications via:

- A. Viatores shared secret information file
- B. Any standard 3rd-party authentication server, such as MS Active Directory, RADIUS, and LDAP, and
- C. Mutual authentication using IPSec Internet Key Exchange (IKE)

User specific information is stored locally on the client device when the Viatores Manager configures the policy with:

Option 1. To make use of 3rd-party authentication with the option to “enforce user name” at login time as part of item B configuration above. See figure 5.11.1-A for a sample configuration dialog.

Option 2. To use public and private key method to perform mutual authentication between the Server and Client using X.509 digital certificate during the IPSec tunnel establishment phase as part of item C configuration above. See figure 5.11.1-B for a sample dialog of a PKI session generating public/private key on the mobile device prior to submitting it to a Certificate Authority.

With Option 1, the user name enforcement option is stored in the encrypted policy configuration file on the mobile device. At Viatores Client login time, the Client will make sure the user name entered matches with that policy user string before passing on user credential in a secure tunnel to the Viatores Server to authenticate before granting access to the network. Examples in figure 5.11-2 shows that mobile devices configured for Capt. Smith and Lt. Johnson can only be used by them, while laptops configured as placeholders can be used by any authorized users including Capt. Smith and Lt. Johnson as long as the right credential is entered and authenticated by the system.

With Option 2, the user uses the Viatores PKI Client to generate RSA or DSA private key, submit his own corresponding public key to an authorized certificate authority (CA), and eventually import his signed X.509 certificate containing his public key and the certificate the signing CA to complete the operation. During the IPSec IKE key exchange phase, user specific digital certificate



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

is exchanged, as well as his digital signature computed based on his private key, are transmitted to the Server for authentication before the tunnel can be successfully established.

Add New User Group

Group Name: Police_Department

Group Password: *****

General Policies

Server Name: VServer

Default Authentication Scheme: NONE

☒ Allow users to quit Viatores Client

☒ Allow users to save Viatores password

☒ Enforce username integrity at logon

Split Tunneling Policies...

Traffic Control Policies...

OK Cancel

Enforce specific user or share laptop

Figure 5.11-1-A – Specific user name information is stored on the laptop policy



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

The screenshot shows the 'Viatores PKI' application window. The 'Certificate Request' tab is selected. The form contains the following fields and values:

Field	Value
User/VPN Device Name	CaptSmith
Organization	UtahPD
Organization Unit	PD
2-char Country Code	US
State or Province	UT
Locality Name(eg, city)	
Subject Alternative Name	
Public Key Type	<input type="radio"/> DSA <input checked="" type="radio"/> RSA
CA LDAP Host	192.168.40.10
Password	*****
Confirm Password	*****

Below the form is a button labeled 'Generate Certificate Request (PKCS#10)'. At the bottom, a message box displays: 'Message Certificate Request has been generated. Go to ne:'.

Figure 5.11.1-B - User uses Viatores PKI Client to generate user specific private and public keys

In addition, the Viatores Manager allows configuration parameters about a group of users to be stored in the policy and in local files to tailor Viatores Client access enforcement, such as:

- Allow all users in the same group to QUIT the Viatores Client or not. If the option is not to allow, then the Viatores Client will not provide the menu option to leave the program
- Allow the users in the same group to save Viatores Client password or not after first successful entry. This provides the system administrator an option to force the user to enter specific Viatores Client password each time he uses the Viatores Client to gain access to the network.



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

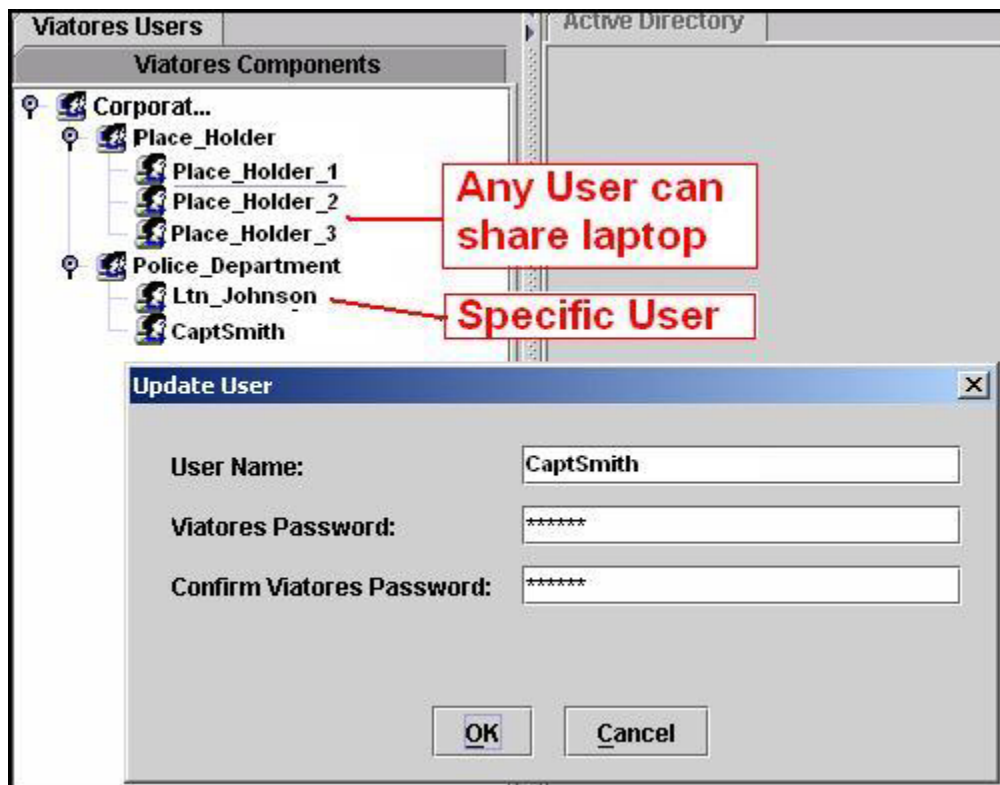


Figure 5.11-2 – Specific user policy or shared mobile device policy

Any Viatores user can modify options such as:

- A) “Search for Wi-Fi hotspot Zone” for public access.
- B) Change the LOG mode to see more or less traffic detail.
- C) Change the network switching prioritization to better fit the user environment (see section 5.19 for more information).

Figure 5.11-3 shows such a dialog for user setting update.

One particular setting that requires specific system administrator permission is “Split-tunneling”. This option must be specified in the policy by the system administrator before the Viatores Client allows the user to update (for example: Add, Edit, Remove) split-tunneling rules. The split-



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

tunneling rule capability is primarily used to allow splitting of non-critical traffic such as:

- Printing to a local printer (with a specific IP address, protocol and port number) while maintaining a secure tunnel to the enterprise network, or
- Maintaining traffic with a particular news web site to obtain out-of-band and useful information that is authorized by the system administrator

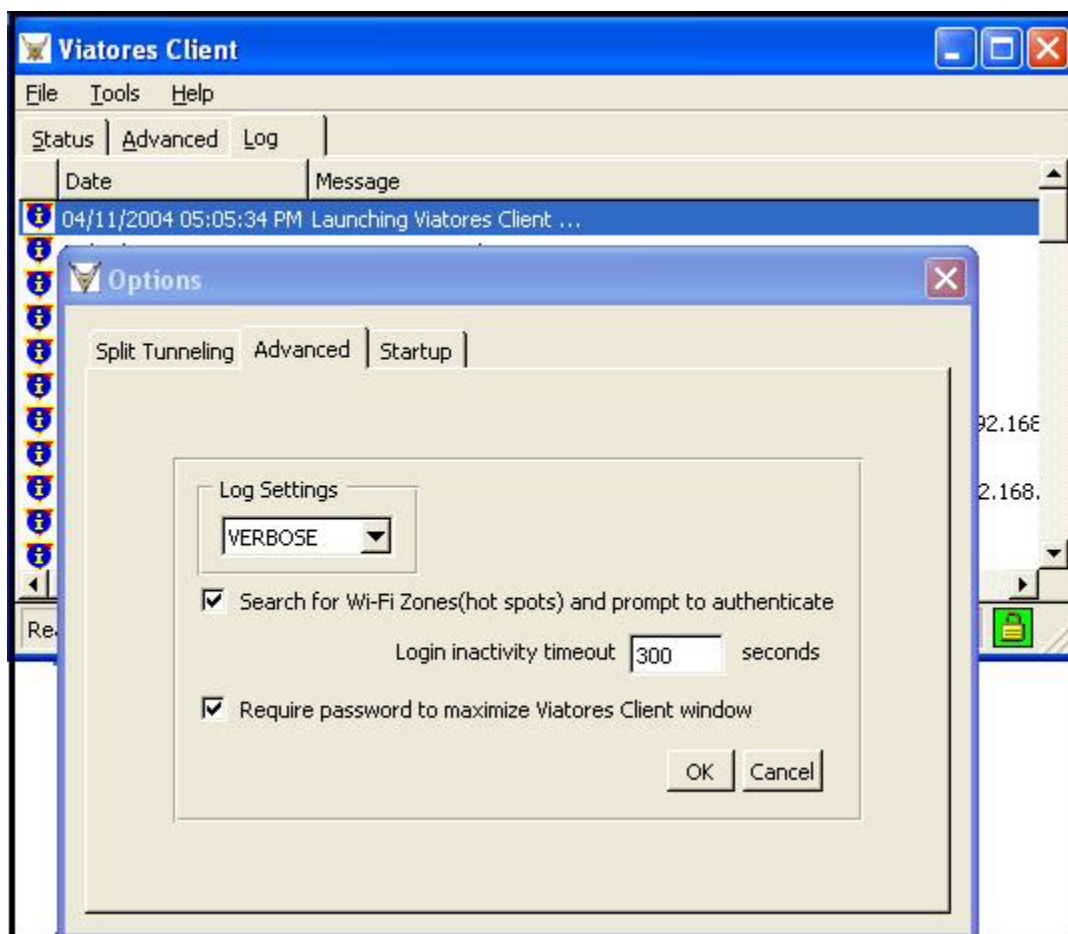


Figure – 5.11-3 - User option to increase log level to VERBOSE mode and automatically detect public hotspot zone



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

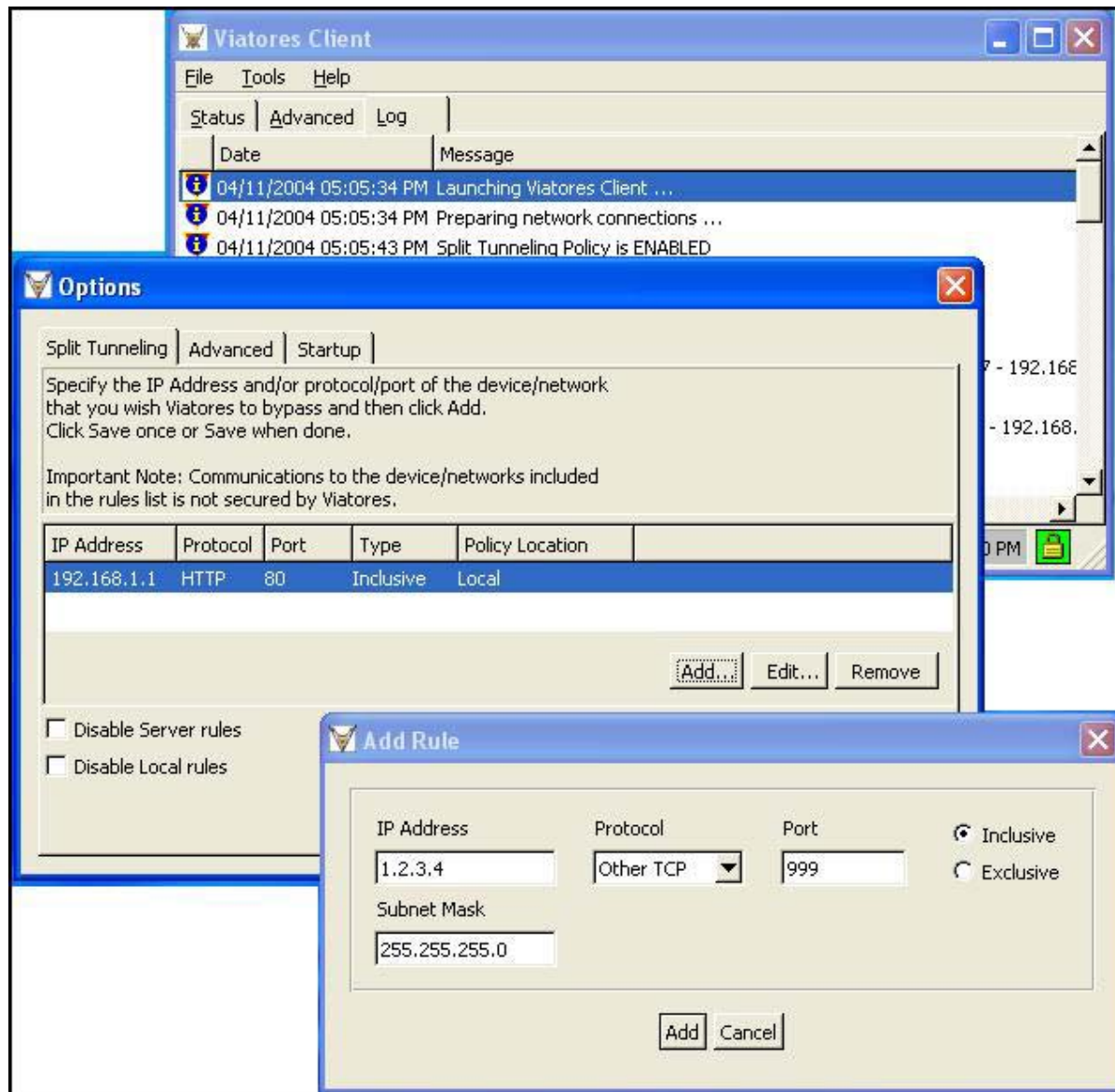


Figure 5.11-4 – Client specifies split traffic if so permitted by the system administrator



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services
S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services
DOUGLAS RICHINS
Division Director

5.14 Revision to Question:

Are there custom implementations required where Novell Netware clients are in use? What steps, if any, are required to bring the laptop into compliance, so the network persistence software will function on these laptops? Is there additional software, which must be loaded, or is there software that must be removed from these laptops?

Ecutel response:

In the Microsoft TCP/IP stack, the Novell Netware Client runs as a protocol service over the IP network layer, while the Viatores Client runs as a tunneling protocol layer below the IP network layer – see figure 5.14-1. Each Novell Netware packet is in TCP/UDP format and therefore can be tunneled successfully by the Viatores protocol driver. Example in figure 5.14-2 shows that the Viatores Client provides a secure tunnel over Wi-Fi, while the Novell Client allows the user to log in and map network drives residing on the Netware Server.

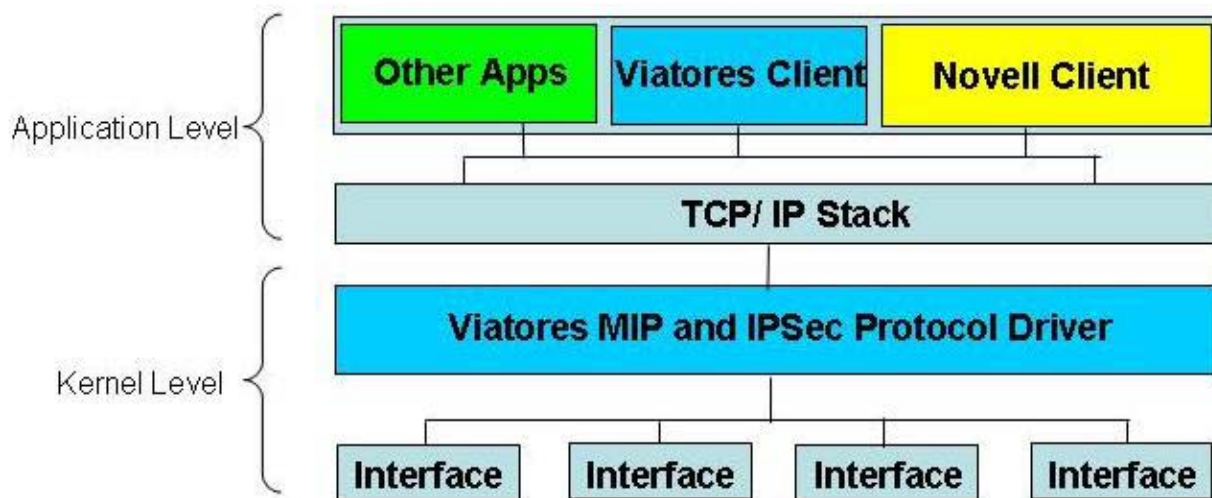


Figure 5.14-1 – Layering in MS TCP/IP stack



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services
S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services
DOUGLAS RICHINS
Division Director

It should be noted that the Novell network login process allows 2 options:

- 1) Log in the workstation or laptop using standard Microsoft local credential or domain credential.**
- 2) Log in the Novell Netware tree and server as part of the Netware single sign-on process.**

If Option 1 is used, there is no custom implementation or additional software required of the Novell Client or the Viatores Client to allow secure access to the Microsoft or Novell network resources, which is shown here in figure 5.14-2. During Viatores Client installation, the system administrator can specify the option run Viatores:

- Manual (user needs to bring up Viatores Client manually from the system menu)**
- Automatic (upon machine login, the Viatores Client is automatically started)**
- Single sign-on to the work MS domain (user will use Viatores specific single sign-on screen)**

Upon login completion, the user can bring up the Novell Client to log into Novell network to access Netware resources.

If Option 2 is used, there is a potential customization such as:

- 1) Chaining of single sign-on operation from the Novell Client to the Viatores Client, via field resource ID passing, to build a secure tunnel to support tunneling of Novell login traffic, or**
- 2) Viatores always-on secure tunnel must be started and established prior to the Novell login process – this may require the Viatores Client and its tunnel to be established automatically upon reboot as the machine main secure tunneling service.**

In Ecutel opinion, there is no additional software needs to be loaded or removed from the laptop.



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

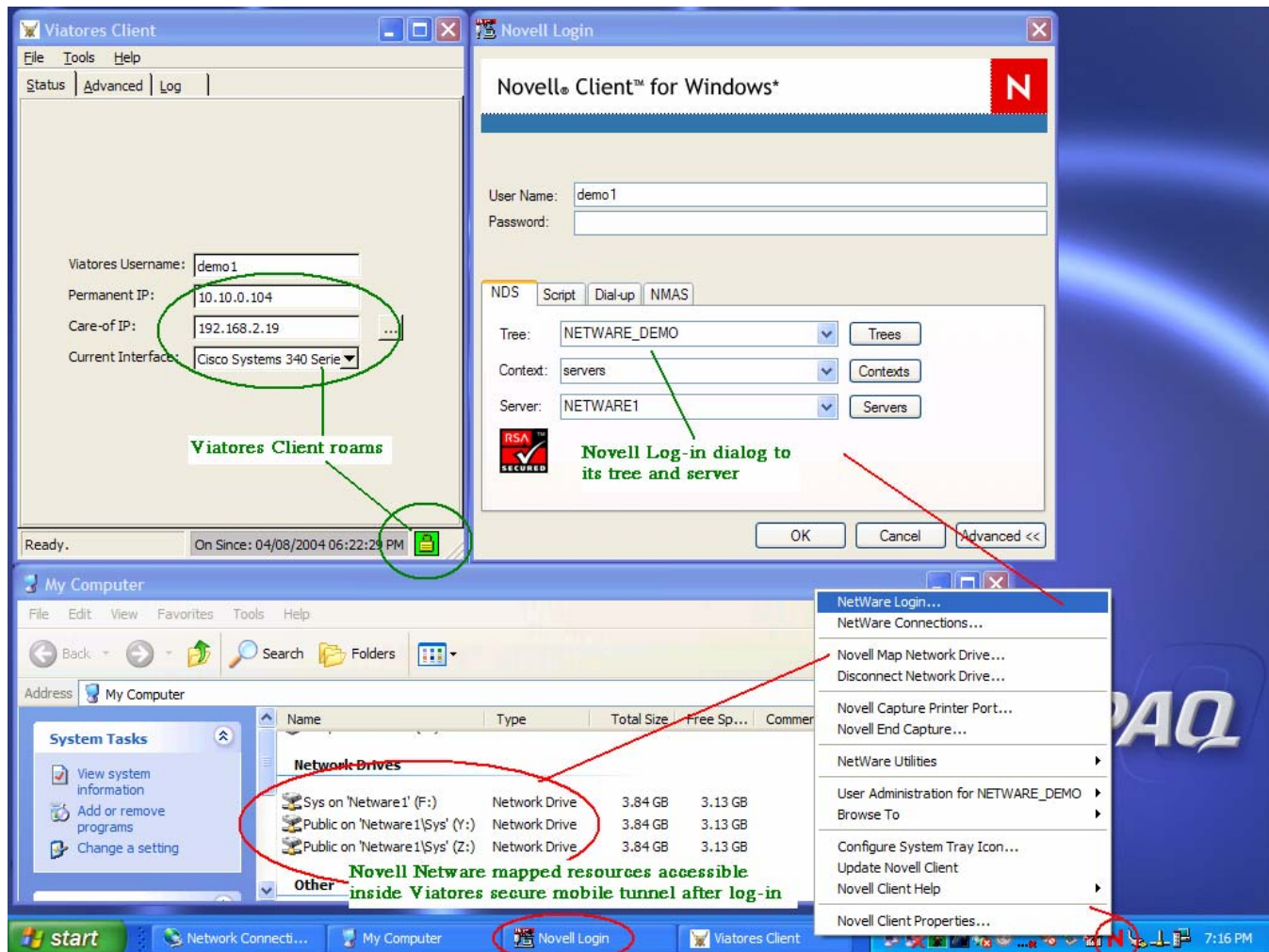


Figure 5.14-2- Viatores Client and Novell Network Client interoperate on the same laptop



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

5.18 Revision to Question:

Some applications, using telnet sessions, need to remain active during network transitions. Please confirm that these types of sessions, as well as other Windows-based applications, will not be disrupted due to the network switching indicated above.

Ecutel response:

The Viatores Client and Server provide network layer persistence and therefore support application level persistence. The Client assigned permanent IP address does not change on the Client Virtual Adapter during roaming and furthermore the same permanent IP address is simultaneously maintained at the Server. The Telnet application, as well as other Windows based application such as Outlook, web search and network mapped drives, will not be disrupted during network roaming from one network to another network because the permanent IP address does not change during such operation. Ecutel has verified and used these applications, and confirms that they survive network switching without having to restart the application.

However, each application protocol has its own built-in time-out value and continuously verifies its own traffic in order to maintain its session. If the laptop roams away from one network to another without having wireless signal or connection and whose disconnect duration is longer than the application's built-in time-out interval, the user application may stop transmitting by itself and therefore has to restarted, or, in some instances, it retries transmitting itself at a late time to reestablish the session.



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services
S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services
DOUGLAS RICHINS
Division Director

5.19 Addendum to Question:

Please explain in more detail how your product prioritizes active network connections, and enables automatic switching to the highest speed network connection.

Ecutel response:

The Viatores Client allows prioritization of communication connections by using the built-in NDIS interface names it recognizes from the system device list. For each network interface that the user installed on the laptop, the system registry will record such a device. The Viatores Adapter List Utility (VALU) can be invoked one time during system installation and configuration to read all communication interface names and lists them in a dialog to allow the user to prioritize. However, the user can run this utility as frequently as when a new interface card is installed. It is not necessary for these cards to be inserted or their connections to be active at the time of prioritization. The selection of network switching preference through the use of heuristic rule by specifying:

- 1) Network connection as LAN or WLAN or OTHER
- 2) Network connection preference or weight in terms of LOW, NORMAL, HIGH

Since there is no reliable or universal means to determine the exact speed of a network based on its connection status to determine if it is of highest or will remain highest speed (i.e. a 10 mbps LAN can run slower behind an ADSL connection than a WLAN if the WLAN is of type 802.11A behind a T-1 line; or a LAN is always more secure and is inside a corporate environment, thus is more preferred to using the WLAN connection which is may be placed outside of the firewall), it is recommended that the user assign the weight of HIGH to a LAN network, the weight of NORMAL to WLAN connections and the weight of LOW to NDIS based wide-area network connections. This heuristic rule in a majority of cases will accommodate network switching based on highest speed network connections that the user can already recognize in advance based on today's technology.

The VALU utility generates network prioritizations in a file called adapter_list.txt – see figure 5.19-1. This text file can easily be transferred to and populated in laptops that have same device types and configurations, thus this process can be created once and reused multiple times without requiring each user to prioritize interfaces individually on each laptop

Each laptop can have multiple NDIS connections and only one PPP connection (Microsoft system limit), the PPP connection defaults to be least preferred due to its traditional use is



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

associated for low speed networks. The prioritization for PPP based connection is always lower in priority than any other NDIS connections and is not necessary to be listed in the adapter_list.txt. Whenever a laptop has an active PPP connection at the same time with an active NDIS WLAN or LAN connection, the laptop will prefer to choose the NDIS WLAN or LAN over the PPP connection until all NDIS connections are disconnected or unattached.

During the actual use or roaming, if a card is inserted or enabled as part of Plug-n-Play, the Viatores Client can match such device name against this adapter_list.txt and recognizes its priority relative to other active connections to make proper network switching decision. Therefore it is not necessary for users to prioritize each connection each time it is active, thus reduces the chance of errors and increases user acceptance.



State of Utah

OLENE S. WALKER
Governor

GAYLE McKEACHNIE
Lieutenant Governor

Administrative Services

S. CAMILLE ANTHONY
Executive Director

Purchasing and General Services

DOUGLAS RICHINS
Division Director

The screenshot shows the Viatores Adapter List Utility (VALU) v 2.0 window. It contains a table with columns for Adapter Name, Adapter Type, and Adapter Weight. Below the table are 'Create' and 'Cancel' buttons. Below the VALU window is a Notepad window titled 'adapter_list.txt' showing the output of the utility.

Adapter Name	Adapter Type	Adapter Weight
Cisco Systems 340 Series Wireless LAN Adapter	WLAN	Normal
Sierra Wireless GPRS Adapter	WLAN	Normal
Sony Ericsson Wireless WAN Adapter	Other	Low
Sierra Wireless AirCard 555 Adapter	Other	Low
Ericsson DSSS Wireless LAN PC Card	WLAN	Normal
Dell TrueMobile 1150 Series Wireless LAN Mini	WLAN	Normal
3Com 3C920 Integrated Fast Ethernet Controller	LAN	High
SMC EZ Connect USB/Ethernet Series Converter	LAN	High
Bluetooth LAN Access Server Driver	Other	Low

adapter_list.txt - Notepad

```
"Cisco Systems 340 Series Wireless LAN Adapter" 3 0
"Sierra Wireless GPRS Adapter" 3 0
"Sony Ericsson Wireless WAN Adapter" 3 -5
"Sierra Wireless AirCard 555 Adapter" 3 -5
"Ericsson DSSS Wireless LAN PC Card" 3 0
"Dell TrueMobile 1150 Series Wireless LAN Mini PCI Card" 3 0
"3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible)" 1 5
"SMC EZ Connect USB/Ethernet Series Converter" 1 5
"Bluetooth LAN Access Server Driver" 3 -5
```

Figure 5.19-2 – VALU tool and prioritization file to enable run-time network switching